Internal Audit Report

Network Vulnerability
April 2003

Audit Team Members

Sandy Chockey, IT Audit Manager

KPMG LLP

Maricopa County
Internal Audit Department

301 West Jefferson St
Suite 1090
Phx, AZ 85003-2143
Phone: 602-506-1585
Fax: 602-506-8957
www.maricopa.gov

April 10, 2003

Fulton Brock, Chairman, Board of Supervisors
Don Stapley, Supervisor, District II
Andrew Kunasek, Supervisor, District III
Max W. Wilson, Supervisor, District IV
Mary Rose Wilcox, Supervisor, District V

We have completed our FY 2002-03 vulnerability assessment of the County's internal systems and networks in accordance with the annual audit plan approved by the Board of Supervisors. The audit was performed by the Internal Audit Department in conjunction with County Counsel and KPMG LLP Consulting. County Counsel has been involved due to the legal implications associated with maintaining confidential network information. The scope of the audit was to determine if adequate security and controls exist for internal County networks to prevent unauthorized intrusions, that could potentially disrupt or damage County networks.

The highlights of this report include the following:

- Many County systems are accessible from a single location in the County network. Telecommunications is in the process of creating restrictions within the County's network to limit the risk that the entire network can be compromised.
- Many County systems are vulnerable to compromise because they are not configured properly, have unnecessary services enabled, or have not received the most current vendor updates.

Although the detailed issues and recommendations are confidential and protected by attorney/client privilege, we have attached a summary report for your review. Management's written responses will be obtained along with completion dates. We have included in this report the departments impacted by our work.

If you have questions, or wish to discuss items presented in this report, please contact Sandy Chockey at 506-1006.

Sincerely,

Ross L. Tate

Ross L. Tate
County Auditor

Executive Summary

Single Point of Access

Many systems in the County's network can be accessed from a single location in the County network. A malicious user could break into the system in one department, identify and compromise targets throughout the County network or gain access to sensitive information. Telecommunications is in the process of creating restrictions within the County's network to limit the risk that the entire network can be compromised.

Denial of Service

A denial of service attack is the intentional overloading of a system's capacity with the intent to shut it down. The voice response system in the Star Call Center was vulnerable to a denial of service attack. The loss of phone service could result in lost citizen calls, impacting the County's ability to perform mandated services. A vendor update to correct this problem was available. The Star Call Center, as well as all departments, should apply vendor-supplied updates in a timely manner.

Unnecessary Services Enabled

A standard practice in the computer industry is to remove or disable unnecessary services from a system when it is first set up. This practice limits the security risk of the system and improves its processing efficiency. We found many unnecessary services enabled, increasing the risk of compromise. Departments should disable unnecessary services.

Password Controls

Many County systems have inadequate password controls that may allow unauthorized system access. County systems should be protected by an effective password policy, which includes specific instruction for password protocol and testing of password integrity. Weak password controls could allow a malicious user to read and/or modify sensitive information contained within County systems. Departments should strengthen password controls.

Vulnerable Servers

Many County servers are not properly configured and maintained in accordance with industry-standard guidelines. This condition increases the risk of a malicious user gaining access to County systems and compromising sensitive information. Departments should properly configure and maintain servers based on business needs.

System Updates

When vendors become aware of problems with their software products, they routinely issue corrective updates, called patches. These patches reduce the risk of system compromise and are readily available to users. We found that seventy-two per cent (72%) of the systems we tested were operating without the latest patches from vendors. Unpatched systems may allow a malicious user to read and/or modify sensitive information contained within County systems. Departments should apply required patches and stay current with published updates.

Weak Security

We identified several Microsoft Windows systems that were not properly secured. These security weaknesses may allow a malicious user to take control of the system and enable malicious code and/or access sensitive information. Departments should restrict network access of read/write to the local system administrators.

Introduction

Background

The Maricopa County network is comprised of multiple internal networks that facilitate communication between and around County agencies, departments, and systems. External access (from the Internet) to the County network is restricted through a complex series of authentication mechanisms (e.g., demilitarized zones, firewalls, routers, switches, etc.) that are maintained by the Maricopa County Chief Information Office (OCIO). In a previous audit, the Internet Network Security Audit, controls around these mechanisms were evaluated, and recommendations provided, to address the risks associated with unauthorized access from outside the County network.

This audit evaluated the next layer of controls within the County network, effectively assessing internal network vulnerabilities. Since the network spans the entire County, there are a number of locations that an unauthorized individual (or hacker) can attempt to gain access to the County network. A hacker can be a curious employee, a terminated/disgruntled former employee, or someone not necessarily affiliated with the County. To account for these and other cases, this Internal Network Vulnerability Assessment was performed to simulate activities by a hacker who had gained physical access to a County facility, and connected to the internal network.

County Risks

During this audit, over 14,000 active network devices were identified--including, but not limited to, printers, routers, switches, desktops, and servers. This is a relatively large number of network devices (both from a government and private sector perspective), that increase the risk of unauthorized access, especially as more devices are added to the County network. As part of our procedures, we attempted to scan the internal network and isolate the most vulnerable systems. In doing so, we selectively targeted network devices with 10 or more open ports. In addition, we added a number of systems that could easily be exploited, such as systems with blank passwords.

The risk associated with needlessly open ports reaches beyond inappropriate access to sensitive data. It also exposes the County network to a hacker who intends to infect the County with a self-propagating computer virus (or worm)--the result of which significantly degrades County operations that are reliant on network performance and availability. Most recently, the County Internet community witnessed the effect of a self-propagating worm and its ability to dramatically decrease Internet performance. While the County has taken steps to establish areas of isolation, it should also consider creating formal network zones to help isolate or contain potential damage.

A recently released draft report, “The National Strategy to Secure Cyberspace” was published by The President’s Critical Infrastructure Protection Board, and provides strategic, as well as tactical recommendations for securing network infrastructures. The County’s network is comparable in size to many large private organizations, and needs to address security-related risks with the same preventive/detective controls and incident response processes as these

organizations. The recommendations provided in this report are based upon this authoritative source, as well as other generally accepted security standards.

Scope and Methodology

The scope of this audit was to determine if current controls on selected systems within the organizations listed below provide reasonable assurance that unnecessary services have been properly disabled, and computer information systems are properly secured.

- Adult Probation
- Animal Care and Control
- Assessor
- Clerk of the Court
- County Attorney
- E-Government
- Environmental Services
- Facilities Management
- Flood Control
- Housing Department
- Human Services
- ICJIS
- Justice Courts
- Juvenile Probation
- Library
- MCDOT
- MIHS
- Planning and Development
- Public Defender
- Public Health
- Recorder
- Sheriff
- Superior Court
- Telecommunications
- Treasurer

Over 160 recommendations were made to these organizations. Eighty percent (80%) have already corrected the issues identified. We appreciate the excellent cooperation received from all those involved with this review.

This audit was performed in accordance with generally accepted government auditing standards.